Management Tool Makes the Connection

Program helps units maintain reach-back capability by monitoring bandwidth requirements.

The U.S. Defense Department is developing software that will allow commanders to quickly design, prepare for deployment, manage and monitor joint task force communications networks. Once connectivity is achieved, the platform-independent system will provide bandwidth management and information assurance capabilities.
Establishing and maintaining communications links is a key aspect of information-centric warfare. As the U.S. military evolves into a more agile force reliant on rapid maneuver and dispersed formations, the ability of units to coordinate operations becomes paramount. Future deployments involving several or all of the services will require seamless contact among units within a theater of operations and assets located in the United States.
Creating a tool to guarantee fluid military connectivity is the goal of a program headed by the U.S. Army's Communications-Electronics Command (CECOM), Fort Monmouth, New Jersey, and the Science Applications International Corporation (SAIC), McLean, Virginia. The joint network management system (JNMS) will provide a deployed task force with a scalable communications planning and management capability that is more flexible than are current applications.
According to George Fitzpatrick, JNMS project leader, warfighter information network-terrestrial program, CECOM, the system is designed for regional commanders in chief (CINCs) and their service components to support joint task forces (JTFs). It will operate between larger national data infrastructure assets such as the secret Internet protocol routing network (SIPRNET), the nonsecure Internet protocol routing network (NIPRNET), and tactical battlefield communications.
With the JNMS, planners can design a network quickly and determine its logistics. It would outline the scope, details, magnitude and logistics needed for a system so that only the right communications and data gear are transported and enough bandwidth is available, he explains. Once the task force is established in its theater of operations, the JNMS then provides network security and spectrum management. It also conducts monitoring, trouble ticketing and fault identification. The system becomes a critical connectivity tool at this level because it must allow continuous communications between task force commanders and their superiors. "It doesn't matter how well you're passing traffic if you can't get it up through SIPRNET or NIPRNET because of a bad connection," Fitzpatrick says.
While the package is being developed by the Army, he notes that it will be used across the entire Defense Department to provide CINCs and their service components with a high-level planning capability. The JNMS project creates common planning and monitoring tools that will collaborate over a distributed network. Once it is operational, staff can monitor the network through every phase of the deployment.
Because the JNMS will provide a standard platform for system planning and monitoring in the theater, personnel will not have to learn new network architectures every time they become part of a JTF, Fitzpatrick explains. Many of the software processes will be

automated—a capability that does not fully exist today. The JNMS will replace the joint defense information infrastructure control system-deployed (JDIICS-D) as a management and planning tool. While JDIICS-D has a variety of features, it is not an integrated capability nor does it possess high-level or detail-level planning or spectrum management functions. “We’ll be adding a lot of capability that is not out there right now for the joint task force commander,” he says.

Scott Rodakowski, SAIC’s JNMS program manager, notes that the technology will provide JTF commanders with the ability to reach back to U.S.-based information assets such as the Defense Information System and the Global Information Grid while extending command and control down to tactical communications networks. The system also has a network operations aspect. Though designed for network management and possessing the tools necessary to plan, control and monitor a network, it also features information dissemination management and information assurance functions.

The JNMS is not hardware dependent. It is entirely software-based. Fitzpatrick notes that the services can host the package on any of their platforms as long as the hardware meets the program’s minimum requirements. Although Fitzpatrick believes each of the services will modify its JNMS suites to meet its specific needs, they all will continue to share a common commercial software package.

A key JNMS program requirement is for a scalable, modular, and easily upgradeable structure to accommodate changing technologies. “You don’t want an architecture that is tied up with a bunch of interdependent modules because every time you remove one, you’re affecting the entire system. We wanted a reasonably open architecture,” Fitzpatrick explains. This flexibility allows the services to avoid problems associated with aging legacy equipment and software, he says. “One of the mandates handed down in the operational requirements document was that the Defense Department basically wanted a commercial system. It was recognized that the military was to follow the private sector, and you might as well take advantage of the monitoring and trouble-ticketing technologies already out there. There’s no sense in developing a unique military system, so the mandate was to use commercial products wherever possible.”

As the key contractor for the program, SAIC is tasked with combining a variety of software types into a single package. According to Rodakowski, in addition to working with legacy military communications networks, the firm must integrate state-of-the-art commercial networking technologies such as Internet protocol router networks and wireless technologies into the JNMS. Very sophisticated commercial applications will be used to help planners design, manage, monitor and reconfigure a network, he says.

All of the JNMS modules will share certain common base-line applications. One major underlying program is the Informatica Power Center, a data integration framework that provides information mapping and sharing among disparate applications. For example, if a government spectrum-planning program needs to share data with a commercial application in the network, Informatica will pass the knowledge on through the system’s core, which is built around an Oracle 8i database. The JNMS will employ a standardized World Wide Web-based graphic user interface that will allow personnel to access various applications. High-level and detail-level planning and engineering monitoring functions will use more specialized interfaces.

Information assurance and security capabilities are an integral feature within the JNMS. The software has data classification levels and applications to separate and encode

information for classified and general use. The initial release of the package will have an intrusion detection capability that will allow commanders and signal personnel to identify unauthorized entries into the network. An additional function allows commanders to access information at all classification levels within the JNMS.

Bandwidth management is another critical issue for a joint task force. Rodakowski notes that in the field, a JTF will use whatever connectivity it can allocate, from ultrahigh frequency networks to combat network radio systems or the Army's tactical internet. In the future, this will extend to technologies such as the military strategic tactical and relay satellite communications system as well as to commercial satellite networks. "What JNMS must do is plan for the use of these communications capabilities, and in monitoring their use, help commanders use their bandwidth efficiently," he says.

SAIC is incorporating a program called Neural Star within the JNMS to manage the efficient use of constrained and limited bandwidth in a theater. Other functions provide the ability to view the network structure and track traffic through specific gateways, Rodakowski observes. Administrators will be able to monitor the network down to the server level to determine which applications are being used efficiently. This function is performed by quality of service programs that will gauge network optimization. He notes that some aspects of the monitoring capability will operate in real time.

Fitzpatrick believes the program's main challenge will be meeting the delivery schedule. Carrying out the software integration involves gathering the commercial and government products, translating them through Informatica and testing the entire package in a limited amount of time. However, he adds that the program's key performance thresholds are not difficult to reach. "We wanted to make an achievable system so we could get it out there quickly. But there are still going to be challenges in integrating commercial products regardless of how established they are. It just takes time," he says.

Rodakowski concedes that integrating legacy and new applications will be a challenge. He notes that an old program may define radio transmissions one way, while newer technology may describe it differently. SAIC will use its data integration framework and Informatica to mesh the programs without significantly altering them. Some functions must be conducted on commercial applications, while other communications models are unique to the military, Rodakowski says. Therefore, it will be necessary to add icons and rules for those particular communications and data models. Modifying commercial programs should be relatively simple because they are designed to adapt to varying international broadcasting standards, he says.

The JNMS program initially will focus on key performance base lines and developing minimum requirements, which SAIC will then integrate into the system's architecture. Qualification testing is planned for 2002, and the first packages are slated for delivery to the military in 2003. Depending on the budget, additional performance thresholds will be added yearly, Fitzpatrick says. —HSK